

WHAT C4SAM IS

One platform for security, automation and IT operations — self-hosted.

C4SAM is not another point solution. It is a **central platform that consolidates security- and operations-relevant functions** — asset discovery, vulnerability management, SIEM, automation, compliance and AI — into one modular architecture with a shared data basis. **Existing systems are integrated, not replaced:** C4SAM connects to the tools you already run and replaces only where it demonstrably saves cost.

~40

Integrated open-source and proprietary components, centrally maintained

100%

Self-hosted — on-premises, private cloud or MSP-operated

0

Vendor lock-in — open standards, documented interfaces, exit-ready

AT

Developed and supported in Austria, EU legal framework

Platform modules

Modular — deployable individually or as a full stack



Asset Discovery & CMDB

Agent- and network-based discovery, segment assignment, lifecycle tagging, business-criticality mapping. Native CMDB as the single source of truth.



Patch, Config & Workflow Automation

Orchestration via SaltStack: patch rollout with verification, quarantine logic, escalation paths, self-healing and drift correction.



Compliance & Reporting

Control mapping for NIS2, ISO 27001, GDPR and DORA. Immutable audit trails, evidence export, scheduled governance reports.



AI Layer & Cpt.SAM

LLM gateway for cloud and local models with per-team budgets. Cpt.SAM queries live platform data via the C4SAM MCP server under the same RBAC.



Vulnerability & Threat Detection

Rule- and behaviour-based detection (Wazuh, Zeek, Suricata), continuous scanning, True Risk Priority scoring across IT, OT, and IoT.



Log Consolidation & SIEM

Normalization of Syslog, Beats, Winlog, NetFlow and SNMP into a unified schema. Correlation rules, alert deduplication, case merging.



Observability & Service Health

Service checks from ICMP to full HTTP, hypervisor and system metrics, network infrastructure — unified in cockpit and service tree. Early warnings before storage, certificates, disks or network cause outages; the service tree pinpoints the root cause.



Certificate Lifecycle

Automated discovery, issuance, renewal and deployment — public CAs and internal PKI, without internet dependency. Built for 47-day validity.

Detection & response pipeline

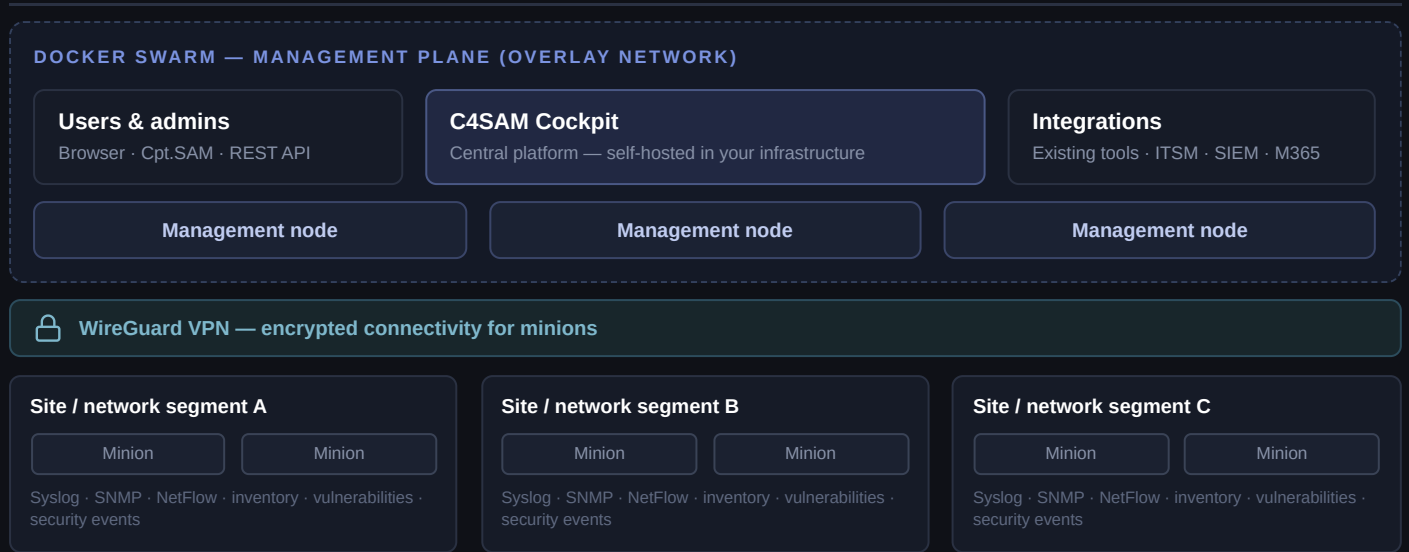
Identical across IT, OT and IoT

01	02	03	04	05	06	07	08
Events	Rules	Alerts	Enrichment	Cases	Triage	Response	Evidence
Logs, NetFlow, telemetry	Detection logic	Signals that matter	Asset, owner, exposure	Related alerts merged	True Risk Priority	Playbooks, isolation	Audit trail

● **See** Collect and detect ● **Assess** Add context and prioritize ● **Act** Respond automatically ● **Prove** Evidence for audits

Deployment architecture

Docker Swarm management plane · WireGuard transport



Scales horizontally by adding management nodes and minions. Multi-tenant across sites, subsidiaries or MSP clients, with per-tenant data separation and delegated administration.

Interfaces & integration

Open standards, documented APIs

Ingest	Syslog (RFC 3164/5424), Beats, Winlogbeat, NetFlow/IPFIX, SNMP v2c/v3, WMI, SSH, agent-based collectors
Identity	LDAP, Active Directory, SAML 2.0, OIDC, SCIM provisioning, MFA (TOTP, WebAuthn)
Outbound	REST API (OpenAPI 3), Webhooks, SMTP, Syslog forwarding, S3-compatible object storage for archives
Ecosystem	ITSM and ticketing systems, third-party SIEM, firewalls and NAC, Microsoft 365 and Entra ID, hypervisors and cloud APIs
AI	C4SAM MCP server, OpenAI-compatible endpoints, locally hosted models (no data leaves the deployment)

Compliance coverage

Technical measures and evidence, out of the box

NIS2 / NISG 2026	Asset inventory, risk management, incident detection and 24/72h reporting workflows, supply-chain register, management reporting
ISO/IEC 27001	Annex A control mapping, evidence collection, internal audit trail, deviation tracking
GDPR	Data minimisation by self-hosting, access logging, retention policies, EU-only processing
DORA	ICT risk register, resilience testing evidence, third-party dependency mapping

Deployment options

No integration project required

 On-premises Bare metal or virtualised, fully air-gapped operation supported.	 Private cloud Your own tenancy on any provider — no shared C4SAM SaaS.	 Managed by MSP Multi-tenant operation with per-client separation and delegated admin.
--	--	---

Enterprise-grade open source, operated for you. Components such as Elastic Stack, Wazuh, Zeek and SaltStack are integrated, hardened, orchestrated and kept current by C4SAM — with a defined lifecycle and support status per component, so you gain the capability without carrying the integration burden.